

## TITLE OF THE INVENTION

### PROCESS FOR CONTROLLING A SWITCHED FULL-DUPLEX ETHERNET TYPE COMMUNICATION NETWORK

#### CROSS REFERENCE TO RELATED APPLICATIONS

**[0001]** The present patent document is a divisional of U.S. application serial No. 10/287,912 filed on November 4, 2002, and claims priority to French patent application FR 01 14263 filed November 5, 2001, the entire contents of each of which are hereby incorporated herein by reference.

#### BACKGROUND OF THE INVENTION

##### FIELD OF THE INVENTION

**[0002]** This invention relates to a process for controlling a switched full-duplex Ethernet type communication network, particularly in avionics.

##### DESCRIPTION OF THE RELATED ART

**[0003]** The Ethernet network, which is the reference in the world of communication networks, can be used to send data in digital form by packets or "frames", where a packet is defined as being a set of data sent in a single step on the network.

**[0004]** In an Ethernet network, the data in each packet are not interpreted. The network carries the data without understanding their meaning. A packet is composed of two types of data, network data that are used to route the packet to its correct destination, and useful data which comprise the "useful load" in the packet.

**[0005]** An Ethernet network is composed of different equipment that is subscribed to the network, and connected to each other through a communication means formed of active equipment called switches, which perform three functions:

**[0006]** connect network subscribers in point to point mode through physical links, which are physical supports for messages to be transferred, for example twisted pair cables,

**[0007]** route (switch) packets sent by source equipment to one or more destination equipment,

**[0008]** check the integrity and the format of the Ethernet packet.

[0009] FIG. 1 illustrates an Ethernet network composed of two switches 11 interconnected to each other and each connected to three items of subscriber equipment 12 in point to point mode.

[0010] Operation of such a network is simple. Each network subscriber can send packets in digital form at any time towards one or several other subscribers. When a switch receives the packets, the "network information" data are analyzed to determine the destination equipment. The packets are then switched towards this equipment.

[0011] In the "switched full-duplex Ethernet type network" expression:

[0012] the "full-duplex" term means that the subscriber can send and receive packets at the same time on the same link,

[0013] the "switched" term means that the packets are switched in switches on appropriate outputs.

[0014] For example, this network may be a 100 Mbits/s switched full-duplex type network on twisted pair; the term "twisted pair" means that connections between the equipment and the switches are composed of two pairs of cables, each pair being twisted; the term 100 Mbits/s simply means the transmission or reception speed of packets on the network.

[0015] The Ethernet technology imposes:

[0016] a minimum size and a maximum size on the packets,

[0017] an identification of the source and/or the destination(s) in each packet,

[0018] a CRC ("Cyclic Redundancy Check") that checks the integrity of the transported data.

[0019] At the present time, in the civil aeronautics field, data exchanges between the various onboard computers are based on the use of the ARINC 429 aeronautical standard.

[0020] However, the switched full-duplex Ethernet network is frequently used in industry.

The emergence of new communication technologies shows that this type of network is an open and standard solution (IEEE standard 802.3) with a considerable potential for development as a local network. But this type of solution does not provide any means of guaranteeing segregation and transfer performances (in terms of network access, latency, etc.) necessary for avionics applications.

## SUMMARY OF THE INVENTION

[0021] The purpose of this invention is to propose a process for controlling a switched full-duplex Ethernet type network, which guarantees data segregation and a limit to data transfer time, to enable application in avionics.

**[0022]** The invention relates to a process for controlling a switched full-duplex Ethernet type network comprising at least one source subscriber equipment and at least one destination subscriber equipment connected to each other through at least one physical link through at least one switch and through at least one virtual link which is the conceptual representation of a link from a source equipment to at least one destination equipment, characterised in that each source equipment transmitting Ethernet frames comprises:

**[0023]** means of segregation between virtual links and allocation of a passband for each virtual link,

**[0024]** means of multiplexing virtual links on the physical link output from this equipment, each transmitted frame having a field that identifies the virtual link to which it belongs.

**[0025]** Advantageously, each destination equipment comprises means of subscribing to at least one virtual link in reception and achieving segregation between virtual links as far as the application.

**[0026]** Advantageously, each switch comprises incoming passband control means for each virtual link. It uses a static configuration table to know which virtual links it needs to switch, and the allowable number of packets for a virtual link. It comprises:

**[0027]** means of separately configuring each input port in order to indicate the output ports towards which each received Ethernet frame must be directed as a function of the virtual link identifier,

**[0028]** means of monitoring the flow of Ethernet frames associated with each virtual link that passes through the switch,

**[0029]** means of reformatting the flow in each virtual link,

**[0030]** means of multiplexing flows in virtual links on each output port.

**[0031]** In one example embodiment, each switch comprises the following in sequence:

**[0032]** an input port,

**[0033]** flow control means,

**[0034]** a switching motor supporting multideestination transfers,

**[0035]** flow control means,

**[0036]** flow reformatting means,

**[0037]** virtual link multiplexing means,

**[0038]** an output port.

**[0039]** Advantageously, a virtual link is characterized by:

**[0040]** a transfer direction, the virtual link being single directional,

**[0041]** a single transmitter subscriber: in this case the equipment,

**[0042]** one or several subscribers in reception: in this case the equipment,

**[0043]** a fixed passband (maximum number of packets per second and their size),

**[0044]** a maximum guaranteed time for transfer of packets from a source equipment to a destination equipment, regardless of the behaviour of the rest of the network, each virtual link having its own transfer time,

**[0045]** a path fixed on the network,

**[0046]** an unique identifier.

**[0047]** In one advantageous embodiment, network redundancy is achieved by doubling up the network, each subscriber having a connection to each of the two networks.

**[0048]** The invention also relates to a process for controlling a switched full-duplex Ethernet type communication network comprising source and destination subscriber equipment connected to each other through at least one physical link through at least one switch and through at least one virtual link that is the conceptual representation of a link from a source equipment to at least one destination equipment, characterized in that in a transmission service, an application is allowed to access virtual links in transmission, this service being used to multiplex virtual links to the physical link through an Ethernet interface, and to send packets for each virtual link as a function of the passband allocated to the virtual link. In a reception service, the packets are decoded, it is checked that their format is correct and useful data are made available to applications. In a passband protection service in the switch, the time characteristics of the packets are checked for each incoming virtual link, and if the allowable characteristics are exceeded, packets are destroyed to prevent a failure at a transmitter or a virtual link from compromising traffic in other virtual links output from this switch.

**[0049]** Advantageously, in one network redundancy service at subscriber level, a packet is sent and received in two virtual links in order to set up network redundancy, duplication of the network that is transparent for applications to guard against a failure in a switch or an interface.

**[0050]** Advantageously, in a "sampling" service, the destination terminal only presents the last received value to the user, and in this service the last value is systematically overwritten by the new received packet. In a "queuing" service, the destination equipment presents all data that it receives to the user, this service making it possible to:

**[0051]** send information that the addressee does not want to lose,

**[0052]** send data larger than the maximum packet size on the virtual link, the transmission service then breaking this data down into packets, and the reception service putting the data together again to make them available to the receiving application.

**[0053]** In a "file transfer" service, a data file is transferred and the transmission service breaks this file down into packets which are then transmitted sequentially, and the reception service recreates this file.

**[0054]** Advantageously, a passband and an inter-packet time are assigned for each virtual link.

**[0055]** In one advantageous embodiment, a subscriber in reception refines the selection of packets on the same virtual link using the network addressing information contained in the packet.

**[0056]** Advantageously, data integrity is achieved on each packet by a CRC that carries out a calculation to validate data transmitted in the packet, each packet is verified at each equipment entry on the network, and every bad packet is destroyed so that it is not used in order to release the passband and thus avoid uselessly creating congestion at the switches.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0057]** A more complete appreciation of the present invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

**[0058]** FIG. 1 illustrates an Ethernet network according to known art,

**[0059]** FIG. 2 illustrates the concept of a virtual link in an Ethernet network according to the invention,

**[0060]** FIG. 3 illustrates an Ethernet network in which several virtual links according to the invention are shown,

**[0061]** FIGS. 4A shows the composition of a transmission equipment, and FIG. 4B shows the composition of a reception equipment, for the network according to the invention,

**[0062]** FIG. 5 illustrates the different component elements of a switch in the network according to the invention,

**[0063]** FIGS. 6 and 7 illustrate different services used in the network according to the invention,

[0064] FIG. 8 illustrates the location of "sampling", "queuing" and "file transfer" services with respect to the application and virtual link services as illustrated in FIGS. 6 and 7, in the network according to the invention,

[0065] FIG. 9 illustrates two examples of packet distributions in a sequence,

[0066] FIG. 10 illustrates the filtering function in a virtual link in reception according to the invention,

[0067] FIG. 11 illustrates an example of a transfer time for a virtual link VL1 according to the invention,

[0068] FIG. 12 illustrates an example verification of the packet in the virtual link VL1 in FIG. 11 according to the invention,

[0069] FIG. 13 illustrates the decomposition of the useful load of a packet in an example embodiment of the network according to the invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0070] The switched full-duplex Ethernet network according to the invention uses the virtual link concept to limit the end to end transfer time, in other words from a source equipment to one (or several items of) destination equipment.

### Concept of Virtual Link

[0071] This virtual link (VL) concept provides means of isolating data transfers between a source equipment 13 and destination equipment 14. A virtual link VL is seen as a "pipe" on the network, as illustrated in FIG. 2.

[0072] A virtual link VL is characterized by:

[0073] a transfer direction, the virtual link being single directional,

[0074] a single source equipment 13,

[0075] one (or several items of) destination equipment 14,

[0076] a fixed passband (maximum number of packets and their size per second),

[0077] a maximum guaranteed time for transfer of packets from a source equipment 13 to a destination equipment 14, regardless of the behavior of the rest of the network, each virtual link having its own transfer time,

[0078] a path fixed on the network,

[0079] an unique identifier.

[0080] A network subscriber may comprise several virtual links VL1, VL2, VL3, as shown in FIG. 3. We have:

[0081] a virtual link VL1 from equipment 21 to equipment 23, 24 and 25,  
 [0082] a virtual link VL2 from equipment 21 to equipment 22 and 23,  
 [0083] a virtual link VL3 from equipment 23 to equipment 22,  
 [0084] When equipment 21 wants to send a packet to equipment 23, 24 and 25, it sends a packet on the virtual link VL1. When it wants to send a packet to equipment 22 and 23, it sends a packet on the virtual link VL2.  
 [0085] The difference between virtual links VL1 and VL2 is identified by the destination identifier in the packet. On the network, the virtual link to which a packet belongs is determined by the identifier of the virtual link in the packet.  
 [0086] A switch uses a static configuration table to determine the virtual links that it is required to switch, and the allowable number of packets for a virtual link.  
 [0087] The virtual link concept is a means of fixing communications between equipment by configuring routes and passbands allocated to the virtual links. Thus, the flow formed by a virtual link is sure to be not disturbed by other flows sharing the same physical links all along its route in the network.  
 [0088] Furthermore, the virtual link concept enables central flow management, to make sure that the sum of the passbands allocated to virtual links on the same physical link does not exceed the capacities of the technology of this physical link. In the above example, the sum of the passbands of virtual links VL1 and VL2 must be less than the transmission capacity of the physical link from equipment 21.  
 [0089] In the network according to the invention, each equipment comprises:  
     [0090] means 32 that define virtual links in transmission and that allocate passbands by controlling segregations,  
     [0091] means 33 that sequence accesses of virtual links to the physical link, in transmission,  
     [0092] means 34 that make it possible to subscribe to one or several virtual links in reception, and that enable segregation between virtual links as far as the application.  
 [0093] FIGS. 4A and 4B represent these means in transmission and in reception respectively, between an application 30 and a physical layer Ethernet controller 31; the complete assembly of means 32 and 33 forming a communication stack 35 and the means 34 forming a communication stack 36.  
 [0094] In the network according to the invention, each switch comprises:

[0095] means of separately configuring each input port in order to indicate the output ports towards which each received Ethernet frame must be directed as a function of the virtual link identifier,

[0096] means of monitoring the flow of Ethernet frames associated with each virtual link that passes through the switch,

[0097] means of reformatting the flow in each virtual link (re-separation of frames for each virtual link),

[0098] means of multiplexing flows in virtual links on each output port.

[0099] Therefore as illustrated in FIG. 5, this switch includes the following in sequence:

[00100] an input port 41,

[00101] flow control means 42,

[00102] a switching motor supporting multideestination transfers 43,

[00103] flow control means 44,

[00104] flow reformatting means 45,

[00105] means of multiplexing the virtual links 46,

[00106] an output port 47.

[00107] Thus, as illustrated in FIG. 6, the network according to the invention is characterized by the implementation of several services or means in each of the subscriber equipment 50:

[00108] a transmission service, the role of which is to enable an application 52 to access virtual links in transmission. This service multiplexes virtual links to the physical link 53 through an Ethernet interface 54, and for each virtual link sends packet as a function of the passband allocated to the virtual link.

[00109] A reception service 55 that decodes the packets, verifies that their format is good and makes useful data available to applications.

[00110] In these transmission and reception services, the virtual link may be represented as being a queue, as seen by the application.

[00111] Other protection services are used to guard against some network failures:

[00112] A passband protection service in the switch, which verifies the time characteristics of packets (separation between packets, the consumed passband), for each incoming virtual link. If the allowable characteristics are exceeded, the packets will simply be destroyed to prevent a failure in a transmitter or a virtual link from compromising traffic in other virtual links starting from this switch.

[00113] A network redundancy service 60 at subscriber level, that enables transmission and reception of a packet on two virtual links in order to implement a



network redundancy. Duplication of the network, which is transparent for applications, thus provides protection against a failure in a switch or an interface (but it does not replace redundancy at system level). As shown in FIG. 7, there are also the transmission and reception services 51 and 55 in FIG. 6, and a network transmission reception redundancy service 60 to which is connected to a first Ethernet interface 61 and to a second Ethernet interface 62.

### Transmission and Reception Modes

**[00114]** The communication interface may supply three additional services to subscriber level applications:

**[00115]** "Sampling": the destination equipment only presents the last received value to the user. In reception, the last value is systematically overwritten by the new received packet. This service is suitable for receiving periodic information.

**[00116]** "Queuing": destination equipment presents all data that it receives to the user, even if the receiver does not read them quickly enough. This service is useful for:

**[00117]** sending information that the addressee does not want to lose (all packets will be read),

**[00118]** sending data larger than the maximum size of the packet on the virtual link. The transmission service then breaks these data down into packets. The reception service reformats the data to make them available to the receiving application.

**[00119]** "File transfer": this service transfers a data file.

**[00120]** The transmission service breaks it down into packets which are then transmitted sequentially. The reception service reconstructs the file. It is also capable of restarting on error (for example in the case of a data download).

**[00121]** FIG. 8 illustrates the location of these services with respect to applications and services on virtual links, using the same references as in FIG. 6.

### Transmission of Packets on a Virtual Link

**[00122]** The invention does not only relate to the definition of virtual links that are used in equipment to send and receive data. It also relates to a particular use of the allocated passband, and sub-filtering functions on reception in a virtual link.

**[00123]** 1) The Allocated Passband and Inter-packet Time

[00124] The allocated passband is defined as being the number of packets sent per second and the size of each packet. But this definition is incomplete because a passband does not give the distribution of these packets in time. It is also necessary to specify the minimum time to be respected between two packets. This minimum inter-packet time (IPT) gives the maximum passband of the virtual link for a given packet size.

[00125] FIG. 9 thus illustrates two example packet distributions in a sequence 70:

[00126] a distribution 71 of 10 packets separated by 1 bit,

[00127] a uniform distribution 72 of 10 packets. The fact of indicating that the minimum inter-packet time is 100 ms gives the maximum traffic envelope on this virtual link, and the passband can be deduced from the packet size using the following formula:

$$[00128] \frac{\text{Packet Size}}{\text{Minimum inter-packet time}} = \text{passband of virtual link}$$

[00129] The assignment of a passband (PB) and an inter-packet time (IPT) for a virtual link does not mean that the packets will systematically be transmitted on the virtual link every IPT and occupy the entire allocated passband. These packets will only be sent on the virtual link when a subscriber application makes them available to the transmission in this virtual link.

[00130] 2) The Filter Function in a Virtual Link in Reception

[00131] On the same virtual link, a subscriber in reception can refine the selection of packets using network addressing information contained in the packet. This filter mode which uses a virtual sub-links concept gives greater flexibility for the definition and use of virtual links by avoiding the creation of specific virtual links.

[00132] FIG. 10 gives an example of a virtual link that supports a stream of three types of packets (a, b and c). Each subscriber can filter (75) the packets according to its needs (subscriber A1-packet a; subscriber A2-packet b; and subscriber A3-packet C).

#### Performances of the Network According to the Invention

[00133] The performances of the network according to the invention can be broken down in four ways:

[00134] data integrity,

[00135] network availability,

[00136] network determinism,

[00137] end to end routing of data.

[00138] 1) Data Integrity

[00139] Data integrity is achieved on each packet by a CRC (Cyclic Redundancy Check) that enables a calculation to validate data transmitted in the packet. The CRC is located at the end of the packet and it corresponds to all bits in the packet (network information plus useful information).

[00140] In the network a packet is verified at each equipment entry to the network, so that every bad packet can be destroyed so that it cannot be used, in order to release the passband and to avoid unnecessarily overloading the switches.

[00141] 2) Network Availability

[00142] The network is shared by several systems for communications. Therefore its availability has a non-negligible impact on the global availability.

[00143] This availability is increased by network redundancy, that consists of doubling up the network, with each subscriber having a connection to each of the two networks, and one of the two packets being selected on reception.

[00144] This network redundancy enables operation even if a switch or several links are defective.

[00145] 3) Network Determinism

[00146] The network is a deterministic network. This means that any packet belonging to a virtual link for an allocated passband is sure of accessing the network and being transmitted to receiving equipment for a limited latency time (maximum packet transit time).

[00147] For a virtual link, the maximum latency calculation is given by the following formula:

$$\text{Latency time of a virtual link} = T_{aE} + T_{TE} + (N \times T_{TS}) + T_{TR} + T_{AR}$$

[00148] Where

[00149] TTE: crossing time through the communication stack in transmission, corresponding to the time necessary to form packets in the communication services. This time is identical for all virtual links and is dependent on the hardware supporting the application.

[00150] T<sub>AE</sub>: transmission access time. The allocated passband is given in the form of a maximum passband and a minimum time between two consecutive packets (inter-packet time IPT). Since packets are sent in a virtual link asynchronously with regard

to the application, if a packet has just been sent, it will be necessary to wait for a time IPT before accessing the network: thus  $TA_E \leq IPT$  in all cases.

[00151] NS: number of switches through which the virtual link passes,

[00152] TTS: maximum time for a packet to pass through a switch,

[00153] TTR: crossing time in reception through the communication stack, corresponding to the time TTE but in reception. This time includes the packet reception time by the services. It is identical for all virtual links, and it depends on the hardware supporting the application.

[00154]  $TA_R$ : access time in reception. When a subscriber receives a packet, it is made available to the application through a "mail box". As a maximum,  $TA_R = IPT$ .

[00155] The times  $TA_E$  and  $TA_R$  are a result of the asynchronism between the applications and the network in transmission and reception.

[00156] A first estimate will give the following maximum values for a packet transfer time, independently of the virtual links:

[00157]  $TTE = 0.5$  ms

[00158]  $TTR = 0.5$  ms

[00159]  $TTS = 1$  ms.

[00160] In the example illustrated in FIG. 11, in which the references in FIG. 2 are repeated, we have:

[00161] For the virtual link VL1 from equipment 13 to equipment 14 through two switches 11, if the time  $IPT = 5$  ms and the read interval = 1 ms, we have:

[00162]  $TA_E = 5$  ms

[00163]  $NS = 2$

[00164]  $TA_R = 1$  ms

[00165] Latency time for a virtual link = 9 ms.

[00166] 4) End to end Routing of Data

[00167] The network according to the invention creates a single end to end route using virtual links, for each packet.

[00168] At each subscriber, each packet is assigned on transmission to a virtual link predefined by configuration. This packet has an addressing part that contains the identification of the virtual link. This identification is used for routing in the network.

[00169] In the routing of a packet, a service verifies if a packet is authorized to pass through each switch at which the packet arrives. Similarly, on reception, a service checks if the packet belongs to a virtual link authorized in reception. If not, the packet is destroyed.

[00170] FIG. 12 illustrates an example verification of a packet in the virtual link VL1 in FIG. 10. This check takes place at points 80.

#### Example Embodiment of the Network According to the Invention in Avionics.

[00171] In this example embodiment, several characteristics of the network according to the invention have been specified, in order to simplify and standardize the use of this network in avionics.

#### Characteristics of Virtual Links

[00172] 1) Number of Virtual Links

[00173] Three subscriber classes are defined, depending on the number of virtual links in transmission and reception:

[00174] large consumer subscriber,

[00175] medium consumer subscriber,

[00176] small consumer subscriber.

[00177] This type of distribution is given in table 1 at the end of the description.

[00178] 2) Passband in Virtual Links

[00179] Each virtual link has an allocated passband that is given by the minimum inter-packet time (IPT) and the packet size. The IPT is given by the following formula:

$$\text{IPT} = 1 \text{ ms} \times 2^k \text{ where } K \text{ is an integer from } 0 \text{ to } 7;$$

[00180] which gives either 1 ms, 2 ms, 4 ms, 8 ms, 16 ms, 32 ms, 64 ms, or 128 ms.

[00181] By definition, four maximum packet sizes have been defined for each virtual link, namely 16 bytes, 98 bytes, 226 bytes and 482 bytes. This size only indicates useful data for the packet, used by applications directly. Network information data are also taken into account for calculation of the passband.

[00182] In table 2 at the end of the description, the effective passbands on the network for a virtual link are given for each packet size (useful load) and for each IPT time.

[00183] The required transmission passband for equipment on aircraft is low (<400 kbits/s). Thus, an upper bound in transmission is given which is summarized by the rule that the sum of passbands of the virtual links VL in transmission must be less than 5 Mbits/s. Thus, in transmission we can have:

[00184] a subscriber with ten 16-byte virtual links at 2 ms (which gives 3.36 Mbits/s), or

[00185] a subscriber with five 16-byte virtual links at 2 ms and ten 226-bytes virtual links at 16 ms and one 226-byte virtual link at 4 ms (which gives 4.778 Mbits/s).

[00186] In order to allocate a passband to a virtual link, a real need has to be identified in terms of data transmission frequency and volume.

[00187] Margins on the passband are given in two ways, either by duplication of the virtual link, or by an effective margin on the passband of the virtual link. In the latter case, it is possible to:

[00188] allocate a useful size larger than necessary,

[00189] allocate a shorter time IPT, so that the packet transmission frequency can be increased, for example the number of packets per second can be doubled if the time IPT changes from 16 ms to 8 ms,

[00190] a combination of the useful size and the time IPT.

[00191] 3) Virtual Links Mode

[00192] Three transfer modes have been defined above, namely "sampling", "queuing", and "file transfer". In order to facilitate the definitions in the virtual links, each virtual link is used either in "sampling" mode or in "queuing" mode or in "file transfer" mode.

[00193] 4) Filtering

[00194] The possibility of filtering in a virtual link enables some equipment to avoid an excessive number of virtual links in transmission and in reception (if the same transmitter). This means can be used to group several virtual links into a single link and to define "virtual sub-links", the packets being selected by network information contained in the packet. Filtering gives better flexibility on the use of communication "pipes" and enables optimisation of their use.

#### Structure and Format of the Useful Load

[00195] The term "structure" specifies the arrangement of the useful load (data transmitted and received by applications) in the packet.

[00196] The term "format" specifies the type of data (integer, binary, etc.).

[00197] The Ethernet standard does not impose the packet structure and the data format (unlike the ARINC 429 standard); however, the following rules are respected in the example considered.

[00198] As illustrated in FIG. 13, the useful load comprises:

[00199] the functional validity (VF) valid for all data in the packet,  
[00200] the data themselves, coded according to a standard format,  
[00201] the arrangement of the data themselves shall be defined by common agreement between the transmitter and the addressees.

**[00202] 1) Functional Validity**

**[00203]** The transmitter calculates the functional validity, and the receiver or receivers use it to determine the degree of confidence to be assigned to the transmitted packet. The functional validity is coded in the first four bytes of the packet.

**[00204]** The functional validity is the equivalent of "SSMs" used on the ARINC 429 aeronautical standard. However, there are some major differences:

**[00205]** This functional validity is purely functional, in other words it only reflects the state of data determined by the transmitting application, and not the state of resources that support it.

**[00206]** The functional validity may be equal to one of the following values:

**[00207]** NO: "Normal Operation"

**[00208]** NCD: "No Computed Data"

**[00209]** FTF: "Functional Test"

**[00210]** The validity of the resources due to distancing between application and resource cannot be generated by the functional validity.

**[00211] 2) Data Format**

**[00212]** Data are coded in a predefined format, in order to standardize exchanges. This format is as similar as possible to the "computer" format manipulated by compilers and microprocessors, to minimize format transformations to be made by applications.

**[00213]** The selected formats are defined in the coding rule illustrated in table 3 at the end of the description.

**[00214] 3) Data Grouping**

**[00215]** The Ethernet protocol is particularly efficient when transmitted information is relatively long. Therefore, it is very advantageous to group data so that they can be sent all at once to facilitate coherence and integrity.

**[00216]** The data grouping criteria may be as follows:

**[00217]** same transfer mode

**[00218]** same refreshment period

**[00219]** functional affinity

**[00220]** same management of functional validity.

## Network Design and Sizing Procedure

[00221] It is essential to define the subscriber hardware and software architecture, at least from the communication point of view, before carrying out a network design and sizing procedure.

[00222] This involves a system and network architecture design phase that must clearly identify:

[00223] physically interfaced equipment on the bus, apart from redundancy,

[00224] transmission and reception subscriber applications seen by the network,

[00225] virtual links as entirely separate elements of the network architecture with its topology.

[00226] The systems must take account of tests and if necessary define specific virtual links for transferring data to test instrumentation means.

[00227] For each hardware equipment, the following are necessary:

[00228] its identification: module name or equipment name,

[00229] its position in the aircraft architecture.

[00230] The following are necessary for each subscriber application:

[00231] its identification: function name,

[00232] its description: a comment,

[00233] its "mapping" on the hardware equipment in the aircraft architecture,

[00234] the identification of the logical interface.

[00235] Equipment, even equipment external to the aircraft, or a test installation, etc., may support several subscribers each with one or several logical interfaces to one or several sub-networks.

[00236] The following are necessary for each virtual link:

[00237] its identification: name of the virtual link,

[00238] the type of information transmitted in the form of a comment,

[00239] the name of the transmitting application,

[00240] the names of receiving applications,

[00241] its routing on hardware equipment in the aircraft architecture in the form of a list of switches passed through, as identified in the architecture,

[00242] the useful passband (bits/s),

[00243] the packet size: the packet size may be fixed or variable in a virtual link, and the maximum size must be given,

[00244] the time IPT,



[00245] justification of the passband, the packet size and the time IPT,

[00246] the usage mode: for "queuing" mode, it is possible to specify if the packet size is greater than 482 bytes,

[00247] the maximum latency.

[00248] The transmission system is responsible for defining virtual links. The transmission system must make sure that equipment in reception take account of virtual links.

#### Means Used

[00249] A database supports this part of the process and defines:

[00250] the hardware architecture of the system with all resources and wiring,

[00251] subscribers (components) and their "mapping" on the hardware architecture,

[00252] virtual links of the system and their routings.

#### Embodiment of a Communication Stack in an Equipment

[00253] This type of stack must enable every subscriber to interface with the communication network.

[00254] There are three possible approaches for integration of this function in the subscriber equipment:

[00255] an autonomous board satisfying all communication needs and capable of interfacing with the rest of the equipment simply through a bus,

[00256] a list of necessary components and the software that can be integrated into the target equipment,

[00257] a subscriber interoperability specification with its validation plan in order to check that the supplier's development is conform with the specified functional requirements.

[00258] TABLE 1

Subscriber Class	Number of virtual links in transmission	Number of Virtual links In reception
Large consumer	32	128
Medium consumer	16	64
Small consumer	8	32

[00259] TABLE 2

Useful					Real passband on the network			
Byte					16	32	64	128
(to)	1 ms	2 ms	4 ms	8 ms	ms	ms	ms	ms
16	672	336	168 000	84	42	21	10	8 280
	000	000		000	000	000	500	
98	1 328	664	332 000	166	83	41	20	10
	000	000		000	000	500	750	375
226	2 352	1 176	588 000	294	147	73	36	18
	000	000		000	000	5000	750	375
482	4 400	2 200	1	550	275	137	68	34
	000	000	100000	000	000	500	750	375

[00260] 16 ots = 64 Ots<sub>Ethernet frame</sub> - 18 Ots<sub>Ethernet header</sub> - 28 Ots<sub>UDP/IP header</sub> - 2 Ots<sub>Redundancy field</sub>

98 ots = 146 Ots<sub>Ethernet frame</sub> - 18 Ots<sub>Ethernet header</sub> - 28 Ots<sub>UDP/IP</sub> - 2 Ots<sub>Redundancy field</sub> 226 ots = 274

Ots<sub>Ethernet frame</sub> - 18 Ots<sub>Ethernet header</sub> - 28 Ots<sub>UDP/IP header</sub> - 2 Ots<sub>Redundancy field</sub> 482 ots = 530 Ots<sub>Ethernet frame</sub> - 18 Ots<sub>Ethernet header</sub> - 28 Ots<sub>UDP/IP header</sub> - 2 Ots<sub>Redundancy field</sub>

[00261] TABLE 3

Type	Standard format
Character	Signed 8-bit ASCII character (Arinc 653)
Integer	Signed 32-bit integer (Arinc 653)
Unsigned integer	Unsigned 32-bit integer (Arinc 653)
Boolean	Unsigned 32-bit integer with info in LSB
Real	32-bit floating point integer according to

**[00262]** Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the present invention may be practiced otherwise than as specifically described herein.